IN THE CLAIMS:

Please substitute the following claims for the same-numbered claims in the application:

1-17. (Cancelled).

18. (Currently Amended) A method for normalization of traffic data in a network comprising:

~~fragmenting and reassembling packets of said data~~;

dynamically establishing and maintaining a normalization table ~~comprising said packets of said data~~;

receiving a packet of data addressed to an end-system in said network and comprising a fragment of a datagram;

determining if an entry is already contained in said normalization table for said datagram because of earlier received fragments;

if said entry is already contained in said normalization table, determining if any conflicts exist between said fragment and said earlier received fragments;

if a conflict exists, discarding said fragment; and

if said conflicts do not exist, simultaneously transferring said packet[[s]] of said data to a network intrusion detection system and ~~a monitored~~ said end-system~~;~~

~~and~~

~~comparing said normalization table and identifiers of said packets of said data,~~

~~wherein said simultaneous transferring further comprises, when no inconsistencies are detected between said normalization table and identifiers of said packets of said data, said packets of said data are immediately forwarded contemporaneously to said network intrusion detection system and to said monitored end-system~~.

19. (Currently Amended) The method according to claim 18, further comprising establishing information about said packet of said data without storing said data in said normalization table by extracting ~~for each said identifier~~ a header and calculating a length of said fragment ~~packet of said data, wherein said header indicates a length of said packet~~.

20. (Currently Amended) The method according to claim 18, further comprising recording ~~at least a~~ partial and complete receipt of said ~~identifier~~ datagram by a sliding bit-mask which is moved to an offset, until said offset indicates receipt of all data of said datagram ~~said data contained in said normalization table~~, wherein said receipt of said ~~identifier~~ datagram is cleared after a time period which is selected equal or slightly higher than a lifetime of the last fragment of said datagram is received ~~said packet inserted into said normalization table~~.

21. (Currently Amended) The method according to one of the claims 18, wherein at least one of a distance and a path MTU to said ~~monitored~~ end-system in [[a]] said network that is ~~are~~ monitored by said network intrusion detection system ~~are~~ is measured and stored in said normalization table one of before said receiving and upon said receiving ~~the receipt~~ of said packet of said data ~~by~~ addressed to said ~~monitored~~ end-system.

22. (Currently Amended) The method according to claim 18, further comprising retrieving from said normalization table TIME TO LIVE value for said packet of said data and measuring a path MTU for said ~~monitored~~ end-system,

wherein when a contents of said TIME TO LIVE value is lower than a predetermined value, then said TIME TO LIVE value replaces said predetermined value; and

wherein when said path MTU is lower than a size of the data packet a do not fragment FLAG is cleared.

23. (Currently Amended) A method for normalization of traffic data in a network comprising:

~~fragmenting and reassembling packets of said data;~~

dynamically establishing and maintaining a normalization table ~~comprising said packets~~;

receiving a packet of data addressed to an end-system in said network and comprising a fragment of a datagram;

determining if an entry is already contained in said normalization table for said datagram because of earlier received fragments;

if said entry is already contained in said normalization table, determining if any conflicts exist between said fragment and said earlier received fragments;

if a conflict exists, discarding said fragment; and

if said conflicts do not exist, simultaneously transferring said packet[[s]] of said data to a network intrusion detection system and ~~a monitored~~ said end-system; ~~and~~

~~comparing said normalization table and identifiers of said packets of said data,~~

~~wherein said simultaneous transferring further comprises, when no inconsistencies are detected between said normalization table and identifiers of said packets of said data, said packets of said data are immediately forwarded contemporaneously to said network intrusion detection system and to said monitored end-system, and~~

wherein said dynamically establishing and ~~monitoring~~ maintaining comprises adding an aging bit to all entries in said normalization table, wherein said aging bit is set whenever said entries are retrieved from said normalization table.

24. (Currently Amended) The method of claim 23, wherein said dynamically establishing and maintaining further comprises periodically sequentially resetting ~~after a time period~~ said aging bits of all of said entries and deleting any of said entries with previously reset aging bits.

25. (Currently Amended) The method according to ~~one of the~~ claim 24, wherein said dynamically establishing and maintaining comprises periodically sequentially probing after a second time period, at least one of a distance and a path MTU to any ~~said monitored~~ end-systems corresponding to any entries ~~said entries stored~~ in said normalization table and updating said normalization table when said distance and said path MTU have changed.

26. (Currently Amended) The method according to claim 23, further comprising establishing information about said packet of said data without storing said data in said normalization table

by extracting ~~for each said identifier~~ a header and calculating a length of said fragment ~~packet of said data, wherein said header indicates a length of said packet~~.

27. (Currently Amended) The method according to claim 23, further comprising ~~recording at least a~~ partial and complete receipt of said ~~identifier~~ datagram by a sliding bit-mask which is moved to an offset, until said offset indicates receipt of all data of said datagram ~~said data contained in said normalization table~~, wherein said receipt of said ~~identifier~~ datagram is cleared after a time period which is selected equal or slightly higher than a lifetime of the last fragment of said datagram is received ~~said packet inserted into said normalization table~~.

28. (Currently Amended) The method according to ~~one of the~~ claim 23, wherein at least one of a distance and a path MTU to said ~~monitored~~ end-system in [[a]] said network ~~are~~ that is monitored by said network intrusion detection system ~~are~~ is measured and stored in said normalization table one of before said receiving and upon said receiving ~~the receipt~~ of said packet of said data [[by]] addressed to said ~~monitored~~ end-system.

29. (Currently Amended) The method according to claim 23, further comprising retrieving from said normalization table TIME TO LIVE value for said packet of said data and measuring a path MTU for said ~~monitored~~ end-system,

wherein when a contents of said TIME TO LIVE value is lower than a predetermined value, then said TIME TO LIVE replaces said predetermined value; and

wherein when said path MTU is lower than a size of the data packet a do not fragment FLAG is cleared.

30. (Currently Amended) A method for normalization of traffic data in a network comprising:

~~fragmenting and reassembling packets of said data;~~

dynamically establishing and maintaining a normalization table ~~comprising said packets~~;

~~handling said packets of said data by any one of modifying said packets of said data, redirecting said packets of said data, and discarding said packets of said data.~~

receiving a packet of data addressed to an end-system in said network and comprising a fragment of a datagram;

determining if an entry is already contained in said normalization table for said datagram because of earlier received fragments;

if said entry is already contained in said normalization table, determining if any conflicts exist between said fragment and said earlier received fragments;

if a conflict exists, discarding said fragment;

if said conflicts do not exist, determining if said fragment fits a bit mask;

if said fragment does not fit said bit mask, redirecting said fragment; and

if said fragment does fit said bit mask, simultaneously transferring said packet[[s]] of said data to a network intrusion detection system and ~~a monitored~~ said end-system~~; and~~

~~comparing said normalization table and identifiers of said packets of said data,~~

~~wherein said simultaneous transferring further comprises, when no inconsistencies are~~

~~detected between said normalization table and identifiers of said packets of said data, said packets of said data are immediately forwarded contemporaneously to said network intrusion detection system and to said monitored end-system~~.

31-32. (Cancelled).

33. (Currently Amended) The method according to claim 30, further comprising establishing information about said packet of said data without storing said data in said normalization table by extracting ~~for each said identifier~~ a header and calculating a length of said fragment ~~packet of said data, wherein said header indicates a length of said packet~~.

34. (Currently Amended) The method according to claim 30, further comprising recording ~~at least a~~ partial and complete receipt of said ~~identifier~~ datagram by a sliding bit-mask which is moved to an offset, until said offset indicates receipt of all data of said datagram ~~said data contained in said normalization table~~, wherein said receipt of said ~~identifier~~ datagram is cleared after a time period which is selected equal or slightly higher than a lifetime of the last fragment of said datagram is received ~~said packet inserted into said normalization table~~.

35. (Currently Amended) The method according to one of the claims 30, wherein at least one of a distance and a path MTU to said ~~monitored~~ end-system in [[a]] said network that is ~~are~~ monitored by said network intrusion detection system ~~are~~ is measured and stored in said

normalization table one of before said receiving and upon said receiving ~~the receipt~~ of said packet of said data [[by]] addressed to said ~~monitored~~ end-system.

36. (Currently Amended) The method according to claim 30, further comprising retrieving from said normalization table TIME TO LIVE value for said packet of said data and measuring a path MTU for said ~~monitored~~ end-system,

wherein when a contents of said TIME TO LIVE value is lower than a predetermined value, then said TIME TO LIVE value replaces said predetermined value; and

wherein when said path MTU is lower than a size of the data packet a do not fragment FLAG is cleared.

37. (Currently Amended) A program storage device ~~computer program product~~ readable by machine, tangibly embodying a program of instructions executable by said machine to perform a method for normalization of traffic data in a network, said method comprising:

~~fragmenting and reassembling packets of said data;~~

dynamically establishing and maintaining a normalization table comprising ~~said packets~~;

receiving a packet of data addressed to an end-system in said network and comprising a fragment of a datagram;

determining if an entry is already contained in said normalization table for said datagram because of earlier received fragments;

if said entry is already contained in said normalization table, determining if any conflicts exist between said fragment and said earlier received fragments;

if a conflict exists, discarding said fragment; and

if said conflicts do not exist, simultaneously transferring said packet[[s]] of said data to a network intrusion detection system and ~~a monitored~~ said end-system~~;~~

~~comparing said normalization table and identifiers of said packets of said data,~~

~~wherein said simultaneous transferring further comprises, when no inconsistencies are detected between said normalization table and identifiers of said packets of said data, said packets of said data are immediately forwarded contemporaneously to said network intrusion detection system and to said monitored end-system, and~~

~~wherein, when inconsistencies are detected between said normalization table and said identifiers of said packets of said data, said packets of said data are handled by any one selected from modifying said packets of said data, redirecting said packets of said data, and discarding said packets of said data~~.

38. (Currently Amended) The ~~computer program product~~ program storage device according to claim 37, ~~wherein said handling further comprises updating said normalization table by inserting a new entry for a current packet of said data when no existing packet of said data comprising the same said identifier as said current packet of said data inserted in said normalization table~~ wherein said dynamically establishing and maintaining comprises adding an aging bit to all entries in said normalization table, wherein said aging bit is set whenever said entries are retrieved from said normalization table.